UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN RE: CAPITAL ONE CONSUMER DATA BREACH SECURITY LITIGATION	)	MDL No. 1:19md2915 (AJT/JFA)
This Document Relates to CONSUMER Cases	)	

PLAINTIFFS' MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANTS' MOTION FOR PROTECTIVE ORDER REGARDING THE MARCH 5, 2019 SEVERITY 1 INCIDENT

A central allegation in this litigation is Plaintiffs' claim that Capital One failed to adequately protect the data it stored on the Amazon cloud resulting in the March 22-23, 2019, Breach. The March 5, 2019, Severity 1 Incident (hereinafter "March 5th Incident")—which Capital One's Chief Enterprise Services Officer and Chief of Staff to the CEO, Frank LaPrade, described as "[redacted]"[1]—involved Capital One's Cloud Custodian product, a product Capital One created and used to protect information on Amazon's cloud. Despite occurring just two weeks before the breach at issue in this case, and despite involving the same Amazon cloud environment at issue here, Capital One has refused discovery into this issue, calling it "a fishing expedition." [ECF No. 821 at 1]. But the information in Plaintiffs' possession reveals the March 5th Incident was a major event, causing significant disruption at Capital One, requiring Capital One to rebuild thousands of virtual computers and their associated data (referred to as "instances" or "resources"), including instances in the Breach-impacted "card prod" account.

While Plaintiffs have asked, Capital One witnesses have yet to answer how long Cloud Custodian was out of commission, how long the remediation took, or how many employees were

[1] CAPITALONE_MDL_001203412, at 422, attached as **Exhibit 1.**

involved in the response and remediation of the March 5th Incident. Certainly scrambling to address a major issue that "shut down" the entire company easily could have—and in Plaintiffs estimation, did—impact Capital One's ability to detect and prevent the Breach. At minimum, Plaintiffs should be permitted to seek discovery aimed at answering those questions, including from a corporate representative of the Capital One Defendants. Accordingly, Plaintiffs submit this memorandum of law in opposition to Capital One Defendants' Motion for Protective Order Regarding The March 5, 2019 Severity 1 Incident [ECF 820] (the "Motion") and brief in support [ECF 821] ("Def. Mem.").

I. Factual Background

Because this dispute involves technical aspects of Capital One's data security, Plaintiffs' provide this background to provide context for this dispute. Cloud Custodian is:

[redacted]

CAPITALONE_MDL_000115232, Def. Mem. Exh. 3 at 2. Thus, when "[redacted]" Rule 30(b)(6) Deposition of Capital One designated witness Jack Walker 79:9–15, attached as **Exhibit 2**.[2]

[2] Capital One attached to its memorandum pages 87–116 of the Walker 30(b)(6) Deposition. Plaintiffs provide pages 79–86 here.

Notably, while Mr. Walker's testimony suggests that Cloud Custodian works as an alerting system, this is not (or, at minimum, not always) the case. Rather—at least prior to the March 5th Incident—Cloud Custodian was programed to remediate violations of the policies it detected; including via deletion of offending resources. *See* Def. Mem. Exh. 3 at 115232 ("[redacted]"). Indeed, removal of that direct remedial ability following the March 5th Incident was raised by those at Capital One as an area of "[redacted]" CAPITALONE_MDL_000115223, Walker Depo. Exh. 19, attached as **Exhibit 3,** ("[redacted]").[3]

Importantly, Cloud Custodian is an "open source" program developed by Capital One,[4] meaning it is freely available on the internet,[5] and changes to the program could be made by anyone else through the open source community, chiefly via GitHub.[6] This open source process for Cloud Custodian is managed by Capital One's open source program office.[7] Of note, the ModSec WAF at issue in the Data Breach was also an open source tool, and Capital One's Security Incident and

[3] While this increased risk was raised to Mr. Walker, it is noticeably absent from the memorandum provided to the Risk Committee of the Board.
[4] Walker, 81:13–14
[5] https://cloudcustodian.io/
[6] Walker 81:14–83:5.
[7] Walker 82:15–16; Terran Peterson Rule 30(b)(6) Testimony, 117: 7–13, attached as **Exhibit 4**.

Event Management ("SIEM") system,[8] [redacted].[9]

Discovery to date has revealed that the March 5th Incident was a result of Capital One's reliance on open source changes. [redacted],[10] introduced the bug that resulted in the March 5th Incident while he was working for Amazon. CAPITALONE_MDL_001203388, at 391 ("[redacted]"), attached as **Exhibit [[5]]**.

On February 13, 2019, [redacted] change, which contained a bug, was committed to the open source Cloud Custodian repository. Walker Dep. Exh. 17, CAPITALONE_MDL_000115185, attached as **Exhibit 6**. On March 5, 2019, following testing by Capital One on February 28, 2019, in its pre-production environment,[11] Capital One released the new version of Cloud Custodian to its production environment. Walker Dep. Exh. 17, CAPITALONE_MDL_000115185. The "bug" determined that [redacted]

[8] SIEM refers to the process of identifying, aggregating, monitoring, recording and analyzing pertinent log data, alerts, security events or incidents within a real-time IT environment. *See, e.g.*, T. Peterson, 50:17–24 ("[redacted]"). The functionality and robustness of a company's SIEM is critical to breach detection, response, and analysis.

[9] T. Peterson, 60:7–8.

[10] Walker, 83:24–25.

[11] "[redacted]." Walker 96:24–97:2.

[redacted] *Id.* [redacted]

[redacted] *Id.*

Worse still, the redundancy Capital One had built into its AWS systems—having resources deployed in both the AWS East and West regions—[redacted]. Def. Mem. Exh. 3, CAPITALONE_MDL_000115232–233. Thus, engineering teams "[redacted]" *Id.* at 115233.

The March 5th Incident was significant; it resulted in customer impacts to multiple lines of business, and was declared a Severity 1 incident, the highest severity rating possible. Walker 91:6–11; 93:4–20. [redacted]" Def. Mem. Exh. 3, CAPITALONE_MDL_000115232.

As Frank Laprade—the supervisor to Capital One's Chief Information Officer, Rob Alexander—put it: "[redacted]" Exh. 1, CAPITALONE_MDL_001203412, at 422. He continued, noting that the March 5th Incident "[redacted]

[redacted]" Exh. 5, CAPITALONE_MDL_001203388 at 393.

Importantly, this issue, which "shut down" the entire company, and caused thousands of instances to have to be rebuilt, occurred only about two weeks prior to the Breach, on March 22–23.

Critical here, it appears that the very environment at issue in the Breach—the "card prod" environment—had to be rebuilt during the March 5th Incident. *See* Def. Mem. Exh. 8, Grim 130:12-15 ("[redacted]"). Yet, despite (apparently) rebuilding that very environment just before the Breach, Capital One failed to identify or remedy the vulnerabilities that had been in place for years and that would result in the Breach.

II. The Requested Information is Relevant, Proportional, and is Not Duplicative or Cumulative

Capital One argues that it has already provided sufficient information to establish the irrelevance of the March 5th Incident. The evidence developed at this point belies this suggestion and supports Plaintiffs' claim the material is relevant. As a general matter, Plaintiffs' claim that Capital One failed to adequately secure information it moved to the AWS cloud, and such failures led to the Breach at issue in this case.

As set out above, Plaintiffs now know the March 5th Incident was significant, "[redacted]" and that the remediation efforts involved the breached card prod environment. Yet, Plaintiffs are still left to guess as to how long Cloud Custodian was out of service, how long remediation efforts took, how many people were involved in response and remediation, and what specifically in card prod had to be rebuilt, including whether the very

instance at issue in the Breach was also rebuilt—in the same misconfigured, improper way it had been for years.

Specifically, Mr. Grim testified that [redacted]. Def. Mem. Exh. 8, Grim, 133:12-19. However, Mr. Grim did not know [redacted] Grim 133:20–134:1. Further, Mr. Grim could not recall [redacted] Grim 129:24-130:5, [redacted] Grim 140:17–141:13. This certainly raises the question of whether other work that could have detected or prevented the Breach—such as the transition away from the ModSec WAF—was also delayed during this critical timeframe of March 2019. And while Mr. Grim was aware [redacted] Grim 141:22–143:8.

Likewise, while Mr. Walker addressed the March 5th incident in his testimony, he also could not answer [redacted], Def. Mem. Exh. 6, Walker 98:10–12; 101:23-102:2, [redacted], Walker 103:10–19, [redacted], Walker 109:10–16.[12]

[12] Capital One also argues that Plaintiffs could have asked Mr. Alexander about the March 5th Incident. However, Plaintiffs used every minute of their allotted 7 hours with Mr. Alexander, and could have used an additional 7 hours with him, and thus had to cut large swaths of questioning, including that related to this issue, given the sheer volume of issues Mr. Alexander, Capital One's CIO, was involved with.

Accordingly, Capital One's suggestion that Plaintiffs could have or should have questioned prior witnesses about the March 5th Incident and obtained the sought-after information [ECF 821 at 10], is contradicted by the very witnesses they reference. Plaintiffs did ask prior witnesses about the pertinent issues and they did not know the answers.[13]

Importantly, without answers to those questions, Capital One's self-serving argument that the March 5th Incident had "'no' impact on the Cyber Incident" [ECF 821 at 8], is baseless. Indeed, if Mr. Walker did not know how long Cloud Custodian was suspended, how long remediation took, or how many employees were involved in responding to or remediating the issue, then his testimony that the absence of Cloud Custodian had no impact on the Breach is pure self-serving speculation.

Capital One's argument that the March 5th Incident only took hours to fix [ECF 821 at 3, 8] is also undermined by its own documents. A memorandum prepared by management to the Risk Committee of Capital One's Board of Directors dated March 6th, reports that "[redacted]." Def. Mem. Exh. 3, CAPITALONE_MDL_000115233. It then lists several actions to be completed over the next *30 days*, implying the outage lasted for approximately one month. Mr. Walker could not testify regarding [redacted].

[13] And even if the individuals witnesses had provided fulsome testimony regarding the pertinent inquiries—and they clearly did not—testimony in an individual capacity does not relieve Capital One from testifying as to the corporation's knowledge, perceptions, and opinions. *See In re: C. R. Bard, Inc. Pelvic Repair Sys. Prod. Liab. Litig.*, MDL No. 2325 (S.D. W. Va. Apr. 22, 2013) ("A Rule 30(b)(6) designee speaks as the corporation and testifies regarding the knowledge, perceptions, and opinions of the corporation. However, when the same deponent testifies in his individual capacity, he provides only his personal knowledge, perceptions, and opinions.") (citing *United States v. Taylor*, 166 F.R.D. 356, 361 (M.D.N.C. 1996)).

Walker 98:10–12; 101:23-103:19. Moreover, Mr. Grim testified regarding work for other projects that was still on [redacted]. Def. Mem. Exh. 8, Grim 140:17–141:13.

Given this background, Plaintiffs should be able to determine for themselves, based on the actual relevant facts rather than self-serving conclusory speculation, whether the March 5th Incident was sufficiently severe in terms of quantity and length of response and remediation, and dedicated employees, to have diverted resources that otherwise would have been available to detect or prevent the Breach—such as the ongoing transition away from the known-to-be-vulnerable ModSec WAF—as well as the specifics of the March 5th Incident remediation as applied to the card prod account, including whether that remediation involved rebuilding (improperly) the very instance at issue in the Breach just days before the Breach occured.

Finally, some of the requests are not solely aimed at the March 5th Incident, and Capital One makes no arguments why that information should be protected from discovery. For example, Requests 57 and 58, and Topics 5–7 generally seek discovery related to Capital One's use of open source, or "public code repositories"; changes made to such open source tools, including who can make such changes; and the risks and risk assessments associated with using open source tools. [ECF 821-1 at 8; ECF 821-2 at 5–6].[14] Given that Cloud Custodian, the breached ModSec WAF, and Capital One's [redacted] are all built on open source code, these inquiries have great relevance, separate and apart from the March 5th Incident, yet Capital One has not challenged them otherwise.

III. Plaintiffs Could Not Have Included the March 5th Incident in the Original Requests

[14] Pincites to docket materials refer to the pagination implement by the CM/ECF system in the top right-hand corner of the document.

Pretrial Order #1 [ECF No. 3], required Plaintiffs to provide Defendants with their Rule 30(b)(6) Deposition Notice by December 20, 2019. [ECF No. 3 at 15]. Initial objections were to be conferred about with unresolved issues filed with the Court by January 13, 2020. [ECF No. 3 at 18]. The operative original Rule 30(b)(6) Notice was served on January 28, 2020. [ECF No. 821-7 at 8, 10]. All of these dates predate the commencement of document production, much less its substantial completion on July 1, 2020. Accordingly, Plaintiffs cannot reasonably be expected to have included issues related to the March 5th Incident—an incident they would only come to learn of from the document production in this case—in their original Rule 30(b)(6) Notice, as Capital One seems to suggest. [ECF No. 821 at 11–12].

To the extent Capital One argues that leave of court is *per se* required before issuing a second 30(b)(6) notice to a party, it is mistaken. To the contrary, where, as here, a party seeks to take a Rule 30(b)(6) deposition on topics not covered in a previous 30(b)(6) deposition, leave of court is not required. *See Quality Aero Tech, Inc. v. Telemetrie Elektronik GmbH*, 212 F.R.D. 313, (E.D.N.C. May 3, 2002); *accord Hamilton v. Bayer Healthcare Pharmaceuticals, Inc.*, No. CIV-18-1240-C (W.D. Okla. July 22, 2019) ("The Court is not persuaded that leave of Court for a second Rule 30(b)(6) deposition is required…. [A] more functional approach should apply…."); *Mobile Telecomm. Techs., LLC v. Blackberry Corp.*, No. 3:12-CV-1652-M-BK, 2015 WL 12698062, at *4 (N.D. Tex. July 15, 2015) ("Although Plaintiff has already deposed two 30(b)(6) corporate witnesses, Plaintiff need not seek leave for additional 30(b)(6) deposition testimony on topics different from those previously noticed.").

However, if the Court is inclined to find leave required for the Second Notice, Plaintiffs respectfully request that the Court construe Plaintiffs' response as a request for leave and grant leave based on the arguments raised above, which establish that the additional deposition topics

are within the scope of permissible discovery and not subject to limitation under Rule 26(b)(2). *See, e.g., Babcock Power, Inc. v. Kapsalis*, No. 3:13-CV-717-DJH-CHL (W.D. Ky. Dec. 17, 2015) (construing response to motion for protective order as motion for leave to take deposition).

Finally, while during the meet and confer process Capital One raised strenuous objections to the relevance of the March 5th Incident, it did not raise the issue of Plaintiffs needing to seek leave to issue a second Rule 30(b)(6) Notice. For that reason, too, this argument should be rejected.

IV. Conclusion

The March 5th Incident raises issues relevant to this case and appropriate for discovery. This incident "shut down" Capital One just days before the Breach, and resulted in thousands of instances, including those in the to-be breached card prod environment, and potentially including the very instance that was exploited in the Breach, being rebuilt in the days immediately prior to the Breach. Capital One's witnesses to date have been unable to provide answers to many of the pertinent questions posed to them by Plaintiffs regarding this issue, such as how long Cloud Custodian was out of service, how long remediation efforts took, how many people were involved in response and remediation, and what specifically in card prod had to be rebuilt, including whether the resources at issue in the Breach were impacted. Accordingly, Capital One's Motion should be denied and Plaintiffs should be permitted to discover whether the March 5th Incident had the sort of significant impact Plaintiffs believe it had on the Breach.

Dated: September 9, 2020.

Respectfully Submitted,

/s/ Steven T. Webster
Steven T. Webster (VSB No. 31975)
WEBSTER BOOK LLP
300 N. Washington Street, Suite 404
Alexandria, Virginia 22314
Tel: (888) 987-9991
swebster@websterbook.com

Plaintiffs' Local Counsel

Norman E. Siegel
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, MO 64112
Tel: (816) 714-7100
siegel@stuevesiegel.com

Karen Hanson Riebel
LOCKRIDGE GRINDAL NAUEN, P.L.L.P
100 Washington Avenue South, Suite 200
Minneapolis, MN 55401
Tel: (612) 339-6900
khriebel@locklaw.com

John A. Yanchunis
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel: (813) 223-5505
jyanchunis@ForThePeople.com

Plaintiffs' Co-Lead Counsel

CERTIFICATE OF SERVICE

I hereby certify that on September 9, 2020, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system, which will send notice of electronic filing to all counsel of record.

/s/ Steven T. Webster
Steven T. Webster (VSB No. 31975)
WEBSTER BOOK LLP